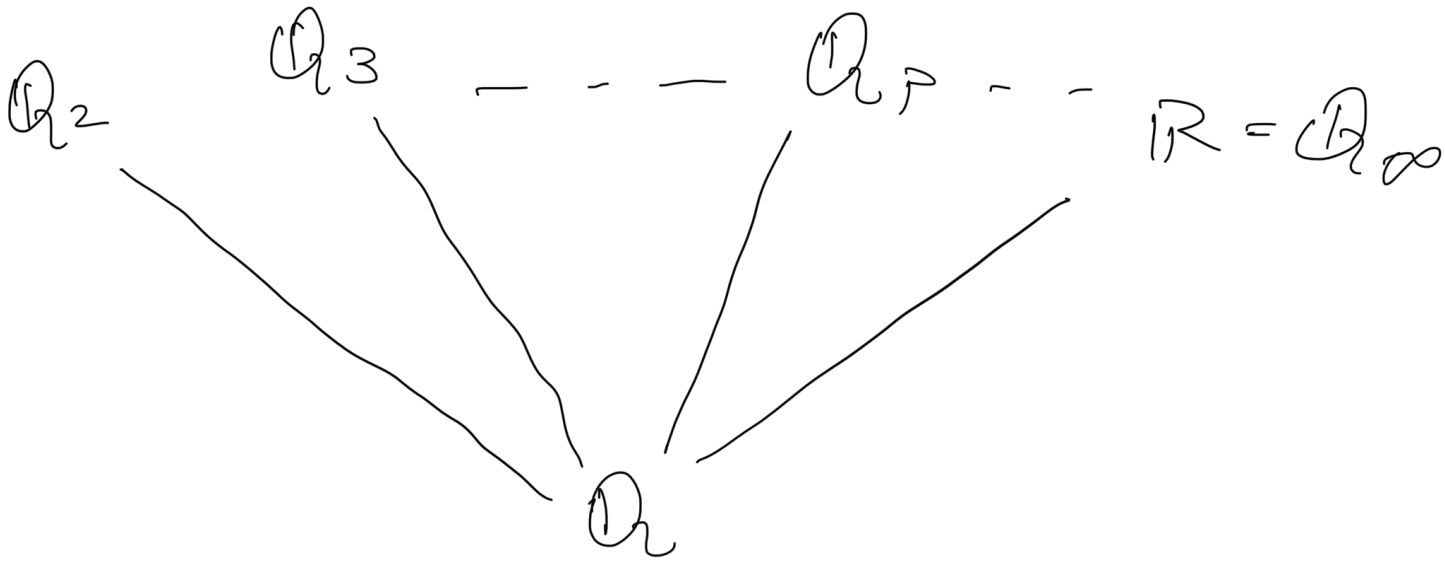
p-adic Numbers



p-adics should be taught before teaching real numbers.

$\mathbb{Q}$ rational numbers

p prime number

We are familiar with absolute value

$$|a-b| = \begin{cases} a-b & \text{if } a-b \geq 0 \\ b-a & \text{if } a-b < 0 \end{cases}$$

distance between two rational numbers

Let us define p-adic absolute value.

For $n \in \mathbb{Z}$

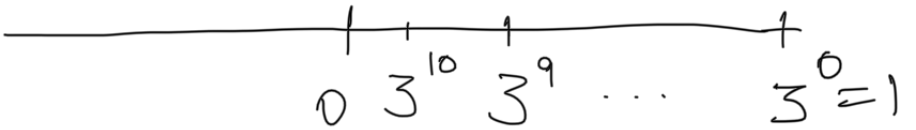
$$n = p^{v_p(n)} n' \qquad p \text{ does not divide } n'.$$

If $a/b \in \mathbb{Q}$ $\quad \gcd(a,b) = 1$

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

$$\left|\frac{a}{b}\right|_p = p^{-v_p(a/b)}$$

$p=3$



Defn: An absolute value on a field K is a function $|\ |: K \longrightarrow \mathbb{R}$ that satisfies

(i) $|x| = 0 \iff x = 0$

(ii) $|xy| = |x|\,|y|$

(iii) $|x+y| \leq |x| + |y|$ (Triangle inequality)

(iv) $|x+y| \leq \max\{|x|, |y|\}$

(Strong triangle inequality)

Absolute values that satisfy only iii) are called Archemedean absolute values.

If iv) holds, they are called non-Archemedean.

For $|\ |_p$

i) $|x|_p = 0 \iff p^{-v_p(x)} = 0$

$\iff v_p(x) = \infty \iff x = 0$

ii) $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x) - v_p(y)}$

$= p^{-v_p(x)}\, p^{-v_p(y)}$

$= |x|_p\, |y|_p$

iv) $|x+y|_p = p^{-v_p(x+y)}$

$x = p^{v_p(x)}\, p'$

$y = p^{v_p(y)}\, p''$

$x+y = p^{\min\{v_p(x),\, v_p(y)\}} \cdot z$

$v_p(x+y) \geq \min\{v_p(x),\, v_p(y)\}$

$|x+y|_p = p^{-v_p(x+y)} \leq \max\{|x|_p,\, |y|_p\}$

iv) $\Rightarrow$ iii)

Examples: If we want to arrange

$$63, \frac{1}{27}, 686, 13929, \frac{243}{3879}$$

in increasing order of 3-adic magnitude, we get

$$\frac{243}{3879} < 63 < 13929 < 686 < \frac{1}{27}$$

Example: A sequence that converges to 0 p-adically is

$$p, p^2, p^3, \ldots, p^n, \ldots$$

Some geometry on $\mathbb{Q}$ (under $|\ |_p$)

Defn: Let K be a field and $|\ |$ an absolute value on K. We define the distance $d(x,y)$ between two elements x and y in K by

$$d(x,y) = |x-y|.$$

(Metric induced by absolute value)

Observe: $|\ |$ is non-archimedean

$\iff$ $d(x,y) \leq \max(d(x,z), d(z,y))$

Lemma: Suppose $|\ |$ is non-archimedean and $|x| \neq |y|$, then

$$|x+y| = \max\{|x|, |y|\}$$

Pf: Assume $|x| > |y|$. Then,

$$|x+y| \leq \max\{|x|, |y|\} = |x|$$

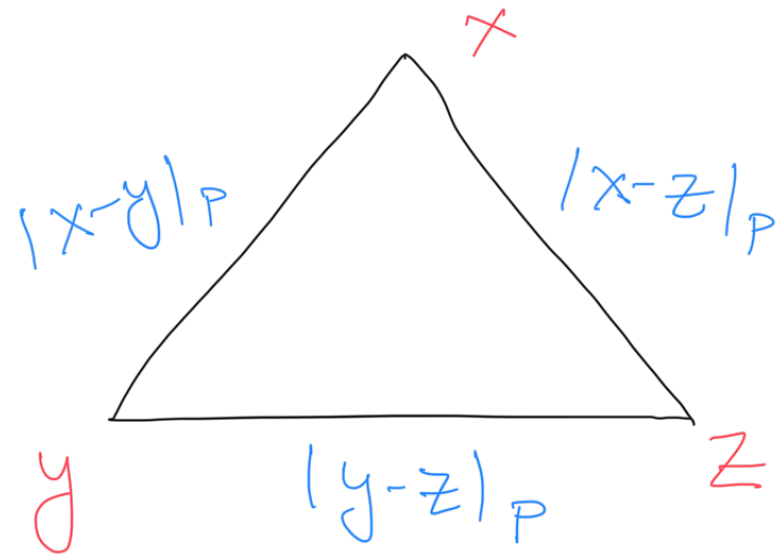
$$|x| = |x+y-y| \leq \max\{|x+y|, |y|\}$$

$$\Rightarrow |x| \leq |x+y|$$

$$\Rightarrow |x+y| = |x| = \max\{|x|, |y|\}$$

Corollary ① All triangles in $\mathbb{Q}$ are isosceles, with respect to $|\ |_p$.

pf:



If $|x-z|_p = |y-z|_p$, then this triangle is isosceles.

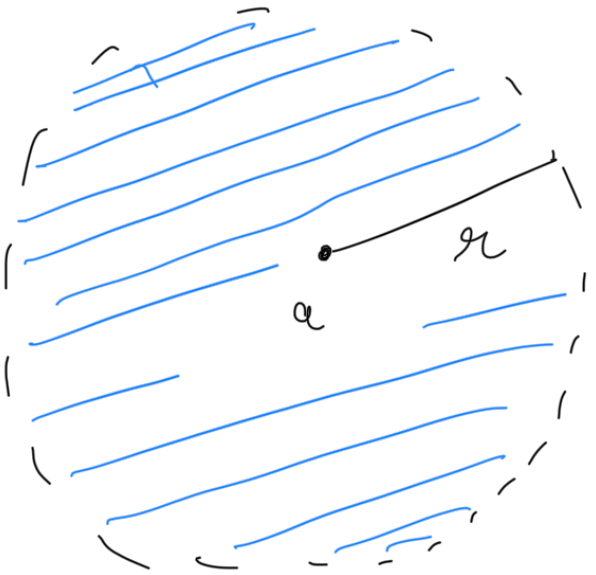
Otherwise assume $|x-z|_p > |y-z|_p$

$$|x-y|_p = |x-z+z-y|_p$$

$$= |x-z|_p$$

$\Rightarrow$ This triangle is isosceles.

Circles in $\mathbb{Q}$ (under $|\ |_p$)



$$B(a,r) = \{ x \in \mathbb{Q} \mid |x-a|_p \leq r \}$$

Proposition: 1) If $b \in B(a,r)$, then

$$B(a,r) = B(b,r).$$

Pf: We will show $B(a,r) \subseteq B(b,r)$

and $B(b,r) \subseteq B(a,r)$.

Proof of $B(a,r) \subseteq B(b,r)$

If $x \in B(a,r) \Rightarrow |x-a|_p \leq r$

$$|x-b|_p = |x-a+a-b|_p \leq \max\{|x-a|, |a-b|\}$$

$\leq r$

$\Rightarrow \quad x \in B(b, r)$

Proof of $B(b,r) \subseteq B(a,r)$

If $x \in B(b,r) \Rightarrow |x-b| \leq r$

$$|x-a| \leq \max\{|x-b|, |a-b|\}$$

$$\leq r$$

$\Rightarrow x \in B(a,r)$.

Every point is the center!

2) $B(a,r) \cap B(b,s) \neq \phi \iff$

$B(a,r) \subseteq B(b,s)$ or $B(b,s) \subseteq B(a,r)$

pf: $\Leftarrow$ is obvious.

$\Rightarrow$: Assume $B(a,r) \cap B(b,s) \neq \phi$

Say $x \in B(a,r) \cap B(b,s)$

$\Rightarrow \quad |a-x| \leq r$ and $|b-x| \leq s$

Assume $r \leq s$

$\forall y \in B(a, r)$

$\Rightarrow |a - y| \leq r \leq s$

$|b - y| \leq \max\{|b - x|, |x - y|\}$

$\leq s$

$\Rightarrow B(a, r) \subseteq B(b, s)$

From $\mathbb{Q}$ to $\mathbb{Q}_p$

Defn: (Cauchy sequences) A sequence $\{x_n\}_{n\in\mathbb{N}}$ is said to be Cauchy with respect to $|\ |$ if for a given $\varepsilon>0$, $\exists\ N$ such that $\forall\ n, m \geq N$

$$|x_n - x_m| < \varepsilon$$

Example: 1) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$

2) $1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \ldots$

↓

Approximations of $\sqrt{2}$

Not every Cauchy sequence in $\mathbb{Q}$ converges to a rational number, when we take Completion of $\mathbb{Q}$ with respect to standard absolute value, we get $\mathbb{R}$.

Similarly, when we take Completion of $\mathbb{Q}$ with respect to $|\ |_p$ we get $\mathbb{Q}_p$.

(In fact, these are all possible absolute values on $\mathbb{Q}$, $|\ |_p$ for a prime p and standard absolute value. (Theorem of Ostrowski))

Qn: Is $\mathbb{Q}$ Complete with respect to $|\ |_p$?

Answer: No!

p odd, $1 < a < p-1$ Consider $\{a^{p^n}\}_{n \geq 1}$

$$|a^{p^{n+1}} - a^{p^n}|_p = |a^{p^n}|_p \, |a^{p^{n+1}-p^n} - 1|_p$$

$$\leq \frac{1}{p^{n+1}}$$

(because $a^{p^n(p-1)} \equiv 1 \pmod{p^{n+1}}$)

But this sequence does not converge to any rational number.

Suppose it does.

$$\lim_{n\to\infty} x_n = x$$

$$\lim_{n\to\infty} x_{n+1} = \lim_{n\to\infty} (x_n)^p = \left(\lim_{n\to\infty} x_n\right)^p$$

$$\Rightarrow x^p = x \Rightarrow x = 1 \text{ or } -1$$

$$\Rightarrow |a-1|_p < 1 \Rightarrow p \mid a-1 \longrightarrow\!\leftarrow$$

$$\text{Or } |a+1|_p < 1 \Rightarrow p \mid a+1 \longrightarrow\!\leftarrow$$

Construction of $\mathbb{Q}_p$

Define $C_p(\mathbb{Q}) = \{ \{x_n\}_{n\geq 1} : \{x_n\}$ is a Cauchy sequence with respect to $|\,|_p \}$

$$\{x_n\} + \{y_n\} = \{x_n + y_n\}$$

$$\{x_n\} \cdot \{y_n\} = \{x_n \cdot y_n\}$$

With addition & multiplication defined as above $C_p(\mathbb{Q})$ is a commutative ring with identity.

Define $I = \left\{ \{x_n\}_{n\geq 1} \;\middle|\; \begin{array}{l} \{x_n\} \in C_p(\mathbb{Q}) \\ \lim_{n\to\infty} x_n = 0 \\ \downarrow \\ \text{with respect to} \\ |\,|_p \end{array} \right\}$

I is an ideal of $C_p(\mathbb{Q})$.

Defn: $\mathbb{Q}_p := C_p(\mathbb{Q}) / I$

$\mathbb{Q}_p$ is not just a ring, it is a field.

It is complete with respect to $|\ |_p$, i.e. every Cauchy sequence in $\mathbb{Q}_p$ converges.

$\mathbb{Q}_p$ is called field of p-adic numbers.

Some algebra in $\mathbb{Q}_p$:

Is $\sqrt{2}$ in $\mathbb{Q}_7$?

$$(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \cdots)^2 = 2 + 0 \cdot 7 + 0 \cdot 7^2 + \cdots$$

$$\Rightarrow \quad a_0^2 \equiv 2 \pmod 7$$

$$\Rightarrow \quad a_0 = 3 \text{ or } a_0 = 4$$

$$(a_0 + a_1 \cdot 7)^2 \equiv 2 \pmod{7^2}$$

$$a_0^2 + 2a_0a_1 \cdot 7 \equiv 2 \pmod{7^2}$$

$a_0 = 3$

$$9 + 6a_1 \cdot 7 \equiv 2 \pmod{7^2}$$

$$6a_1 \cdot 7 \equiv -7 \pmod{7^2}$$

$$\Rightarrow 6a_1 \equiv -1 \pmod{7}$$

$$\Rightarrow a_1 \equiv 1 \pmod{7}$$

$\vdots$

Continue like this

$$(3 + 1 \cdot 7 + 2 \cdot 7^2 + \cdots) = \sqrt{2} \in \mathbb{Q}_7.$$

Exc: Show that $\sqrt{3} \notin \mathbb{Q}_7$.